Unit 15 Warwick Innovation Centre
Warwick Technology Park
Gallows Hill
Warwick
CV34 6UW

ACCEPTABLE USE POLICY (AUP)

Date: 22/06/2026

1. Introduction and Scope

1.1 This Acceptable Use Policy (AUP) sets out the rules governing access to and use of the Values Alignment Index (the Service) provided by And Evolve Limited (the Provider). It applies to the Customer and all individuals authorised by the Customer to use the Service (Authorised Users).

1.2 This AUP forms part of, and is incorporated by reference into, the agreement between the Provider and the Customer governing the Customer's use of the Service (the Agreement). Capitalised terms used but not defined in this AUP have the meanings given in the Agreement.

2. Definitions In this AUP:

2.1 Authorised Users means those people authorised by the Customer to use the Service under this Agreement, in respect of the number of Licences purchased on the Portal.

2.2 Customer Data means any data, content, materials or information supplied, uploaded, or provided by or on behalf of the Customer or Authorised Users to, or processed by the Service for, the Customer, in each case excluding Usage Data.

2.3 Provider Systems means the software, platform, applications, websites, infrastructure, networks, systems, tools, reports, APIs and other technology operated by or on behalf of the Provider to deliver the Service, together with all related intellectual property and proprietary materials.

2.4 Service means the Provider's provision of the measurement of orientation, and then the alignment of people's human values as described in Schedule 2 (Service Description) to the Agreement, and any updates or enhancements thereto made generally available by the Provider during the Term, if any.

3. Permitted Use

3.1 The Customer and Authorised Users may use the Service solely for the Customer's internal business purposes in accordance with the Agreement and this AUP.

3.2 Use is limited to the number of licences purchased and provisioned to named Authorised Users and any applicable usage parameters or limits set out in the Agreement or notified by the Provider from time to time.

4. Prohibited Uses The Customer and Authorised Users must not, and must not permit any third party to:

4.1 Unlawful content and activities: use the Service to upload, store, process, transmit, publish or otherwise make available any content or to engage in any activity that is unlawful, fraudulent or otherwise in breach of applicable law or regulation.

4.2 Intellectual property infringement: use the Service to infringe, misappropriate or violate any intellectual property, proprietary or moral rights of any person, including without limitation unauthorised copying, distribution or public display of third-party

Company Registration No: 9395138 Registered Office: Unit 15 Warwick Innovation Centre, Warwick Technology Park, Gallows Hill, Warwick, CV34 6UW

content.
4.3 Privacy violations: collect, process or transmit personal data in contravention of applicable data protection and privacy laws, or without appropriate notices, consents or other lawful basis.
4.4 Harassment and abuse: use the Service to harass, threaten, defame, bully, stalk or otherwise abuse any person, or to promote or facilitate violence or self-harm.
4.5 Hate and discriminatory content: upload or transmit content that is hateful, discriminatory or that incites hatred or violence against individuals or groups based on protected characteristics.
4.6 Obscene or sexually explicit content: upload or transmit pornographic, obscene or sexually explicit content, or content that exploits or harms minors.
4.7 Malware and harmful code: distribute, create, upload or transmit viruses, worms, Trojan horses, ransomware, spyware, malicious scripts or other code, files or programs intended to interfere with, damage or gain unauthorised access to systems, data or networks.
4.8 Phishing, social engineering and deception: engage in phishing, pharming, spoofing, social engineering, deceptive practices or any activity intended to obtain confidential information or credentials from others.
4.9 Spam and unsolicited communications: use the Service to send or facilitate the sending of unsolicited or bulk communications, advertising or promotional materials not permitted by applicable law, including spam or junk mail.
4.10 Security testing and interference: conduct security testing, including penetration testing, vulnerability scanning, stress testing or load testing of the Service or Provider Systems, without the Provider's prior written consent. 4.11 Unauthorised access: attempt to gain or assist others to gain unauthorised access to the Service, Provider Systems or related networks, accounts or data.
4.12 Credential misuse: share, transfer or otherwise misuse authentication credentials or permit any account to be used by more than one individual, or circumvent named user/per-seat restrictions.
4.13 Circumvention: attempt to bypass, circumvent or disable any security, usage limits, access controls, licensing or metering features of the Service, including attempts to avoid or reduce applicable fees.
4.14 Scraping and data extraction: access or use the Service through any automated means, including bots, scrapers, spiders or crawlers, to harvest, index, mine or extract data, except as expressly permitted by the Provider via documented APIs.
4.15 Reverse engineering: reverse engineer, decompile, disassemble or otherwise attempt to derive the source code, underlying ideas, algorithms or non-public APIs of the Service, except to the extent such restriction is prohibited by applicable law.
4.16 Competitive use and benchmarking: use the Service to develop, train, improve or offer a competing product or service, or to benchmark, compare or publish performance or feature information about the Service without the Provider's prior written consent.
4.17 Interference with service: interfere with or disrupt the integrity, performance or availability of the Service or Provider Systems, including deliberate introduction of

excessive traffic or load.
4.18 Excessive load and misuse: impose an unreasonable or disproportionately large load on the Service or Provider Systems, or otherwise use the Service in a manner inconsistent with normal, intended usage or fair use limits notified by the Provider.
4.19 Misuse of APIs: use the Provider's APIs in violation of published technical documentation, rate limits or access policies, or in a manner that degrades the Service for others.
4.20 Illegal goods and services: use the Service to promote, facilitate or transact illegal goods or services.
4.21 High-risk use: use the Service in any high-risk environment where failure could lead to death, personal injury, or severe environmental or property damage, unless expressly agreed in writing.
4.22 Content moderation evasion: attempt to evade or defeat content or abuse detection, moderation or enforcement mechanisms.

5. Data and Content Responsibilities

5.1 The Customer is solely responsible for the nature, quality, accuracy and legality of Customer Data and for ensuring it does not violate this AUP, the Agreement or applicable laws.
5.2 The Customer must ensure that it has all necessary rights, licences, consents and permissions to submit Customer Data to the Service and to authorise its processing by the Provider in accordance with the Agreement. 5.3 The Customer must not submit any special categories of personal data or other sensitive data unless expressly permitted under the Agreement and processed in accordance with applicable law.

6. Account and Security Obligations

6.1 The Customer must ensure that Authorised Users keep their account credentials confidential and secure and that credentials are not shared between individuals.
6.2 The Customer must implement appropriate administrative, technical and organisational measures to secure access to the Service and to protect Customer Data.
6.3 The Customer must promptly notify the Provider at support@and-evolve.com if it suspects or becomes aware of any unauthorised access to or use of any account, credentials or the Service.

7. Monitoring and Enforcement

7.1 The Provider may monitor use of the Service, including Customer and Authorised User activity, to the extent necessary to operate and secure the Service, to investigate suspected breaches of this AUP or the Agreement, and to comply with applicable law or a lawful request of a competent authority. Where any such monitoring involves personal data within Customer Data, the Provider carries it out as processor, in accordance with the Agreement and the Data Protection Addendum and only to the extent permitted by applicable law. The Provider uses only Usage Data, which does not identify the Customer or any individual, to analyse and improve the Service.
7.2 The Provider may remove, disable access to or modify any content that it reasonably believes breaches this AUP or applicable law.

7.3 The Provider may suspend or restrict access to the Service in accordance with clause 11 (Consequences of Breach).

8. Reporting Security Incidents and Abuse

8.1 The Customer must promptly, and in any event without undue delay, notify the Provider at support@and-evolve.com upon becoming aware of any actual or suspected security incident, vulnerability, unauthorised access, misuse or other breach relating to the Service or Provider Systems.

8.2 The Customer must also promptly report any abuse or suspected breach of this AUP by any user to support@and-evolve.com and provide reasonable detail to support the Provider's investigation.

9. Cooperation with Investigations

9.1 The Customer will reasonably cooperate with the Provider's investigation of any suspected security incident, abuse or breach of this AUP, including by providing relevant logs, records, cooperation of personnel and timely responses to enquiries, subject to applicable law.

9.2 Where required by law or valid legal process, the Provider may disclose information relating to the Customer's or Authorised Users' use of the Service to competent authorities. The Provider will, where lawful, notify the Customer of such disclosure requests.

10. Acceptable Use of Support Channels

10.1 The Customer and Authorised Users must use support channels only for legitimate support requests related to the Service.

10.2 The Customer must not use support channels to transmit unlawful, inappropriate or confidential information not necessary for resolving a support issue, nor to harass Provider personnel.

10.3 The Customer must comply with any support plans, contact routes, ticket limits and response processes communicated by the Provider, including any applicable fair use limits.

11. Consequences of Breach

11.1 Without limiting any other rights or remedies, if the Provider reasonably believes that the Customer or any Authorised User has breached this AUP, the Provider may take one or more of the following steps, acting reasonably and having regard to the nature and severity of the breach: issue a written warning and require remediation within a specified timeframe; temporarily suspend or restrict access for the affected account(s) or features; remove or disable access to offending content; require the Customer to pay reasonable costs of remediation, recovery or repairs incurred by the Provider due to the breach; and terminate the relevant account(s) or the Agreement in accordance with its terms.

11.2 Notwithstanding clause 11.1, the Provider may immediately suspend all or part of the Service without prior notice where the Provider reasonably deems such action necessary to protect the Service, Provider Systems, other customers or users, or to comply with applicable law or a lawful request of a competent authority.

11.3 The Provider will notify the Customer of any suspension and, where practicable,

work with the Customer to resolve the underlying issue to enable prompt restoration of the Service.

12. Compliance with Laws

12.1 The Customer must ensure that its and its Authorised Users' use of the Service complies with all applicable laws and regulations, including those relating to privacy, data protection, electronic communications and consumer protection.

12.2 Export controls and sanctions: The Customer must not access or use the Service in, or for the benefit of, any country or region subject to comprehensive trade sanctions, or by any person or entity on applicable sanctions or restricted party lists, or for any purpose prohibited by applicable export control or sanctions laws. The Customer is responsible for obtaining any required export, re-export or import authorisations.

13. Third-Party Integrations

13.1 Where the Service enables integration or interoperability with third-party products, services, websites or applications, the Customer's use of such third-party offerings is subject to the third party's terms and policies. The Provider is not responsible for third-party offerings and does not control their content or security.

13.2 The Customer must not use integrations to circumvent this AUP, the Agreement or the Service's technical or licensing restrictions.

14. Changes to this AUP

14.1 The Provider may update this AUP from time to time to reflect changes in law, best practice, or to address new risks or features of the Service.

14.2 The Provider will notify the Customer of material changes by email to the contact details held for the Customer or via in-product notice no less than 30 days before the change takes effect, unless a shorter period is required by law or relates to urgent security or abuse matters.

14.3 Continued use of the Service after the effective date of the updated AUP constitutes acceptance of the updated AUP.

15. Contact Details

15.1 Questions, reports of abuse or security concerns relating to this AUP should be directed to support@and-evolve.com.

15.2 The Provider's registered office and additional contact information are set out in the Agreement or as notified to the Customer from time to time.

16. General

16.1 In the event of any conflict between this AUP and the Agreement, the Agreement will prevail to the extent of the conflict, except that this AUP will prevail with respect to acceptable use requirements.

16.2 If any provision of this AUP is found invalid or unenforceable, the remaining provisions will remain in full force and effect.

16.3 Failure or delay by the Provider to enforce any provision of this AUP will not constitute a waiver of that provision.